9-1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/683,507	01/10/2002	Craig H. Rowland	800584	8139

5073 7590 08/25/2005

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)	
Office Action Summary	09/683,507	ROWLAND ET AL.	
	Examiner	**Art Unit**	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _19 November 2004_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-49_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-49_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _10 January 2002_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _see attached_.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statements (IDS) submitted are in compliance with the provisions of 37 CFR 1.97. Accordingly, the examiner is considering the information disclosure statement. The examiner notes that the reference by Jansen et al, entitled "Applying Mobile Agents to Intrusion Detection and Response" has been cited twice, so a line has been drawn through the duplicate citation on the PTO-1449.

Priority

2. Applicant's claim for domestic priority under 35 U.S.C. 119(e) is acknowledged.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-49 are rejected under 35 U.S.C. 102(b) as being anticipated by Jansen et al, entitled "Applying Mobile Agents to Intrusion Detection and Response".

As per claims 1, 30, and 48, it is disclosed by Jansen et al of a computer implemented method for providing system security and resource management. It is taught of managing event messages by a master control processor between system handlers according to security system policies, processing network messages by a network handler between client and server computers, inserting native and third party event messages received by an intrusion handler into the master control processor for processing by other system handlers, detecting and processing event message signatures by the signature handler from alarm, system, and insertion events for conversion into system alarm messages for action by the other system handlers, and performing actions by an action handler in response to action requests from the master control processor (page 2, section 1.2, page 5, section 1.3.6, page 29, section 5.4.3).

As per claims 2-4, Jansen et al teaches of maintaining an execution environment by an agent handler for mobile autonomous code modules, collecting logging event messages by a logging handler, and managing system configuration parameters by a configuration handler (page 2, section 1.2 and page 29, section 5.4.3).

As per claim 5, Jansen et al teaches of registering system handlers, passing event messages between system handlers and managing event queues attached to system handlers (page 29, section 5.4.2).

As per claim 6, Jansen et al discloses of reading a handler module to determine the initialization requirement, initializing the handler application programming interface, determining if the handler is to run as a remote procedure call, making the handler available through the remote procedure call interface if run as a remote procedure call, and initializing the handler input/output queues if not run as a remote procedure call (pages 7-9, section 2.1).

As per claim 7, Jansen et al teaches of system handlers comprising static dynamic system processes (page 9, section 2.2).

As per claim 8, Jansen et al discloses of initiating system handlers by internal mechanisms, external mechanisms, and from the master control processor (pages 2-3, section 1.2).

As per claim 9, it is recited by Jansen et al of system handlers having a reversible architecture to enable the system handlers to be used in either a client or server computer mode (page 26, section 5.2).

As per claim 10, Jansen et al discloses of allowing connection only from clients and servers defined in an access control list, authenticating protocols with client and servers, compressing data to minimize bandwidth requirements, and encrypting data to provide secure communication (pages 7-9, section 2.1).

As per claim 11, Jansen et al recites of reading and writing messages using an insertion method selected from the group consisting of file descriptor, network sockets and named pipe, using native insertion mode library to directly insert messages into the master control processor, and using an external insertion mode library linked to a third party source to directly insert messages into the master control processor (page 5, section 1.3.6).

As per claim 12, Jansen et al teaches of accepting alarm events from the master control processor, decoding the alarm type and originator from the alarm event, consulting internal signature registry for alarms of the type accepted, handling the alarm message off to the signature module for processing, extracting alarm macro information, determining if an alarm has occurred, consulting the action policy if an alarm has occurred to determine response, and passing the resulting response message to the master control processor for action by the other system handlers (pages 7-9, section 2.1).

As per claim 13, Jansen et al teaches of actions performed by the action handler is selected from the group consisting of blocking a host with a modified route command, blocking a host with a packet filter modification command, disabling a user account, disabling a network interface, running an external user-defined command, logging an event, sending email or page alerts, sending on-screen alerts to users or administrators, requesting server executed action, and a pluggable action defined by a user (pages 7-9, section 2.1).

As per claim 14, Jansen et al discloses of receiving event messages containing a signature by the signature handler from the master control processor, detecting an attack by the signature handler from the event message signature, consulting action policy by the signature handler and determining action to be taken by the signature handler, ending the process if no action is required, determining action parameters by the signature handler if action is required, sending an action request to the action handler by the signature handler via the master control processor, processing and executing the action request by the action handler and returning status of the executed action to the signature handler.

As per claim 15, it is recited by Jansen et al of mobile autonomous code modules carry appropriate credentials, are authenticated and cryptographically signed by a trusted introducer, and are able to execute on a host operating system, distributing mobile autonomous code modules to one or more client computers, executing the mobile autonomous code modules without interference, allowing the mobile autonomous code modules to collect and report its results, and shutting down the mobile autonomous code modules (page 5, section 1.3.6 and pages 7-9, section 2.1).

As per claim 16, Jansen et al teaches of verifying detecting alarms, reducing false alarms and providing immediate response (pages 7-9, section 2.1).

As per claim 17, Jansen et al discloses of actively looking for problems and identifying attackers when problems are detected (pages 7-9, section 2.1).

As per claim 18, Jansen et al teaches of performing security and system administration tasks in self-healing network environments (pages 7-9, section 2.1).

As per claim 19, Jansen et al discloses of allowing self-healing components of the system to move between clients and operate independently where required (pages 7-9, section 2.1).

As per claim 20, Jansen et al recites of enabling self-healing and adaptive networks, facilitating distribution of updates for mobile autonomous code modules and centralizing command and control functions for increased reliability (page 5, section 1.3.6 and pages 7-9, section 2.1).

As per claim 21, it is recited by Jansen et al of a peer to peer defensive cluster with mobile autonomous code modules (page 5, section 1.3.6).

As per claim 22, Jansen et al teaches of maintaining an execution environment by the agent handler further comprises protecting the mobile autonomous code modules from alteration or tampering by hostile adversaries, and dispatching the mobile autonomous code modules through a predictable schedule from a central point (page 5, section 1.3.6).

As per claim 23, Jansen et al recites of mobile autonomous code modules are dispatched through a random schedule (page 5, section 1.3.6).

As per claim 24, Jansen et al discloses of programming the mobile autonomous code modules to detect and remove attackers at random, storing code for the mobile autonomous code modules at a central location, preventing alteration of the mobile autonomous code modules with updated security detection strategies without modifying client computers, beginning an active search for attackers when alerted to an intruder's presence, performing automated corrective measures to remove the intruder and saving the forensic evidence (pages 7-9, section 2.1).

As per claim 25, Jansen et al teaches of security specific mobile autonomous modules are selected from the group consisting of forensic evidence agent, intrusion control agent, file integrity agent, host scanning agent, known intrusion agent, loadable kernel module agent, password cracking agent, log archive agent, rootkit agent, suspicious file agent, promiscuous mode agent, hidden process detection agent, unauthorized network daemon agent, self-test agent, spy agent, zombie shells agent, and insider attack agent (pages 7-9, section 2.1).

As per claim 26, Jansen et al discloses of gathering forensic evidence agent from protected systems that are cryptographically signed to prevent tampering (pages 7-9, section 2.1).

As per claim 27, Jansen et al teaches of mobile autonomous code modules are selected from the group consisting of backup agents, host inventory agent, system monitor and status agent, system task agent, and PpatchWatch agent (pages 10-14).

As per claim 28, it is recited in the teachings of Jansen et al of logging event messages by selecting from a group of text-based files, local system auditing facility, cryptographically signed secure log format, directly to a system console, email notification, direct user interface, and system wide notification (pages 7-9, section 2.1).

As per claim 29, Jansen et al discloses of interfacing generic calls to other system handlers, reading, writing, and changing system configuration parameters, reverting system configuration parameters back to a previous version, deleting and backing up system configuration parameters, and providing multiple access protection mechanisms (pages 7-9, section 2.1).

As per claims 31 and 49, Jansen et al recites of an agent handler for maintaining an execution environment for mobile autonomous code modules, logging handler for collecting and logging event message, and a configuration handler for managing system configuration parameters (page 2, section 1.2 and page 29, section 5.4.3).

As per claims 32-36, Jansen et al discloses of system handlers auto-register themselves and their capabilities to the master control processor, an action handler utilizing pluggable action modules, a signature handler utilizing pluggable signature modules, pluggable signature modules auto-register with the signature handler,and pluggable signature modules use stored data from other signature modules, stores data between execution, stores data between system startup and shutdown sequences, and only processes signatures relating to the signature module (pages 28-29).

As per claim 37, Jansen et al teaches of pluggable signature modules are added and removed from the system without modifying the core system code (pages 7-9, section 2.1).

As per claim 38, Jansen et al discloses of installing the system on one server and on client computer (page 26, section 5.2).

As per claim 39, Jansen et al recites of one client operating independently of the system installed on the server for reduced processing and reaction time and when network communications are disrupted (pages 7-9, section 2.1).

As per claim 40, Jansen et al teaches of the use of a graphical user interface (pages 7-9, section 2.1).

As per claim 41, Jansen et al recites of multiple levels of independent alarm filters on the client and server computers for reduced false alarm reporting, configuration flexibility, and system granularity (pages 10-14).

As per claim 42, Jansen et al discloses of encrypting and mutually authenticated communication links between server and client and graphical user interface (pages 7-9, section 2.1).

As per claim 43, Jansen et al recites of reallocating system resources to circumvent system problems or failures (pages 7-9, section 2.1).

As per claim 44, Jansen et al teaches of collecting and forwarding events, processing local client signatures, generating events, initiating and responding to action requests, initiating self-healing counter-measures, and host mobile autonomous code agents (pages 7-9, section 2.1).

As per claim 45, it is disclosed by Jansen et al of collecting and storing events, process enterprise client signatures, generating events, operating a central system database, schedule events, initiating and responding to action requests, initiating self-healing counter-measures, maintaining a graphical user interface backend structure, and manage mobile autonomous code agents (pages 7-9, section 2.1).

As per claim 46, Jansen et al recites of client performing in event of the server failing (pages 13-14, section 3.1.7).

As per claim 47, Jansen et al discloses of the server performing in event of the client failing (pages 13-14, section 3.1.7).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131

8/18/05

CR
August 18, 2005